

1 ARAVIND SWAMINATHAN (*pro hac vice*  
forthcoming)  
2 aswamianthan@orrick.com  
REBECCA HARLOW (STATE BAR NO. 281931)  
3 rharlow@orrick.com  
THOMAS FU (STATE BAR NO. 325209)  
4 tfu@orrick.com  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
5 The Orrick Building  
405 Howard Street  
6 San Francisco, CA 94105-2669  
Telephone: +1 415 773 5700  
7 Facsimile: +1 415 773 5759  
8 Attorneys for Defendant  
Blackhawk Network, Inc.  
9

10 UNITED STATES DISTRICT COURT  
11 NORTHERN DISTRICT OF CALIFORNIA  
12 SAN FRANCISCO DIVISION  
13  
14

15 *IN RE: BLACKHAWK NETWORK DATA*  
16 *BREACH LITIGATION*  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Case No. 3:22-cv-07084-CRB

**DEFENDANT BLACKHAWK  
NETWORK, INC.'S MOTION TO  
DISMISS PLAINTIFFS' AMENDED  
CONSOLIDATED CLASS ACTION  
COMPLAINT**

Date: April 21, 2023  
Time: 10:00 a.m.  
Location: Courtroom 6, 17th Floor  
450 Golden Gate Ave.  
San Francisco, California

Judge: Hon. Charles R. Breyer

**NOTICE OF MOTION TO DISMISS**

**PLEASE TAKE NOTICE** that on April 21, 2023 at 10:00 a.m., or as soon thereafter as the matter may be heard in Courtroom 6 (17th Floor) of the above-entitled court, located at 450 Golden Gate Avenue, San Francisco, California 94102, defendant Blackhawk Network, Inc. (“Blackhawk”) will, and hereby does, move the Court under Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the Amended Class Action Complaint (“Complaint” or “Compl.”) (ECF No. 26) of plaintiffs Steven Pryor, Shane Scheib, Sabrina Singleton, Silvia Cortez, Brian O’Connor, and Kelly Rogers (together “Plaintiffs”). This motion is based on this notice, the concurrently filed memorandum of points and authorities, and all other facts the court may or should take notice of, all files, records, and proceedings in this case, and any oral argument the Court may entertain.

**STATEMENT OF RELIEF SOUGHT (CIVIL L.R. 7-2(B)(3)).** Blackhawk seeks an Order pursuant to Federal Rule of Civil Procedure 12(b)(6) dismissing the Complaint for failure to state a claim upon which relief can be granted.

Dated: March 13, 2023

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: /s/ Aravind Swaminathan

ARAVIND SWAMINATHAN  
REBECCA HARLOW  
THOMAS FU  
Attorneys for Defendant  
Blackhawk Networks, Inc.

## TABLE OF CONTENTS

		Page
I.	SUMMARY OF ARGUMENT (STANDING ORDER I.C).....	VI
II.	STATEMENT OF ISSUES TO BE DECIDED (CIVIL L.R. 7-4(A)(3)) .....	1
III.	SUMMARY OF RELEVANT FACTS .....	1
IV.	LEGAL STANDARD.....	2
V.	ARGUMENT .....	2
A.	The Complaint Fails To State A Claim For Negligence. ....	2
1.	Plaintiffs fail to plead facts showing that Blackhawk was negligent. ....	3
2.	Plaintiffs fail to plead facts showing that they suffered cognizable injury. ....	5
B.	Plaintiffs fail to state a claim for breach of implied contract. ....	9
C.	Plaintiffs fail to state a claim for unjust enrichment. ....	10
D.	Plaintiffs fail to state a claim under the UCL.....	10
E.	Plaintiffs fail to state a claim under the CCPA. ....	11
F.	Plaintiffs fail to state a claim for deceit by concealment. ....	12
G.	Plaintiffs fail to state a claim under various state consumer protection statutes.....	13
VI.	CONCLUSION .....	15

## TABLE OF AUTHORITIES

## Page(s)

**Cases**

<i>Adkins v. Facebook, Inc.</i> , 424 F. Supp. 3d 686 (N.D. Cal. 2019) .....	8
<i>Aguilar v. Hartford Accident &amp; Indem. Co.</i> , 2019 WL 2912861 (C.D. Cal. 2019).....	5
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	2, 3
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	2
<i>Brisson v. Bayer Corp.</i> , 2013 WL 12097794 (S.D. Cal. 2013) .....	12
<i>Corona v. Sony Pictures Ent., Inc.</i> , 2015 WL 3916744 (C.D. Cal. 2015).....	7, 8, 9
<i>Danfer-Klaben v. JPMorgan Chase Bank, N.A.</i> , 2022 WL 3012528 (C.D. Cal. 2022).....	12
<i>Erlich v. Menezes</i> , 21 Cal. 4th 543 (1999) .....	7
<i>In re Facebook, Inc., Consumer Priv. User Profile Litig.</i> , 402 F. Supp. 3d 767 (N.D. Cal. 2019) .....	12
<i>In re Flash Memory Antitrust Litig.</i> , 643 F. Supp. 2d 1133 (N.D. Cal. 2009) .....	11
<i>Floors for Living, LLC v. MAPEI Corp.</i> , 2020 WL 13413204 (S.D. Tex. 2020) .....	14
<i>Gardiner v. Walmart Inc.</i> , 2021 WL 2520103 (N.D. Cal. 2021).....	10
<i>Gardner v. Health Net, Inc.</i> , 2010 WL 11597979 (C.D. Cal. 2010).....	9
<i>In re Google Assistant Priv. Litig.</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020) .....	8
<i>Guajardo v. Skechers USA, Inc.</i> , 503 F. Supp. 3d 746 (C.D. Ill. 2020).....	14
<i>Hayden v. Retail Equation, Inc.</i> , 2022 WL 2254461 (C.D. Cal. 2022).....	4

1	<i>In re iPhone Application Litig.</i> ,	
2	2011 WL 4403963 (N.D. Cal. 2011).....	11
3	<i>Jasso v. Citizens Telecomms. Co. of Cal.</i> ,	
4	2007 WL 97036 (E.D. Cal. 2007).....	3
5	<i>Jordache Enters., Inc. v. Brobeck, Pheger &amp; Harrison</i> ,	
6	18 Cal. 4th 739 (1998) .....	7, 9
7	<i>Keegan v. Am. Honda Motor Co., Inc.</i> ,	
8	838 F. Supp. 2d 929 (C.D. Cal. 2012).....	14
9	<i>Kuhns v. Scottrade, Inc.</i> ,	
10	868 F.3d 711 (8th Cir. 2017).....	4
11	<i>Kwikset Corp. v. Super. Ct.</i> ,	
12	51 Cal. 4th 310 (2011) .....	10
13	<i>Licea v. Caraway Home Inc.</i> ,	
14	2023 WL 1999496 (C.D. Cal. 2023).....	viii
15	<i>LiMandri v. Judkins</i> ,	
16	52 Cal. App. 4th 326 (1997).....	13
17	<i>In re LinkedIn User Privacy Litig.</i> ,	
18	932 F. Supp. 2d 1089 (N.D. Cal. 2013) .....	8
19	<i>Miner v. Gov't Payment Serv., Inc.</i> ,	
20	2015 WL 3528243 (N.D. Ill. 2015).....	15
21	<i>Monson v. Country Preferred Ins. Co.</i> ,	
22	2018 WL 11016704 (D. Colo. 2018) .....	14
23	<i>MyGo, LLC v. Mission Beach Indus., LLC</i> ,	
24	2017 WL 107346 (S.D. Cal. 2017) .....	13
25	<i>Ortiz v. Perkins &amp; Co.</i> ,	
26	2022 WL 16637993 (N.D. Cal. 2022).....	9, 10
27	<i>Papasan v. Allain</i> ,	
28	478 U.S. 265 (1986) .....	2
	<i>Pica v. Delta Air Lines, Inc.</i> ,	
	2018 WL 5861362 (C.D. Cal. 2018).....	4
	<i>Razuki v. Caliber Home Loans, Inc.</i> ,	
	2018 WL 6018361 (S.D. Cal. 2018) .....	3, 4, 10
	<i>Rudgayzer v. Yahoo! Inc.</i> ,	
	2012 WL 5471149 (N.D. Cal. 2012).....	6
	<i>Ruiz v. Gap, Inc.</i> ,	
	2009 WL 250481 (N.D. Cal. 2009).....	11

1	<i>Ruiz v. Gap, Inc.</i> ,	
2	622 F. Supp. 2d 908 (N.D. Cal. 2009) .....	7, 9
3	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
4	2020 WL 2214152 (S.D. Cal. 2020) .....	2
5	<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> ,	
6	996 F.Supp.2d 942 (S.D. Cal. 2014) .....	6
7	<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litig.</i> ,	
8	903 F. Supp. 2d 942 (S.D. Cal. 2012) .....	5, 7, 9, 11
9	<i>Tae Youn Shim v. Lawler</i> ,	
10	2019 WL 2996443 (N.D. Cal. 2019).....	12
11	<i>Terpin v. AT&amp;T Mobility, LLC</i> ,	
12	2020 WL 5369410 (C.D. Cal. 2020).....	13
13	<i>Vess v. Ciba-Geigy Corp. USA</i> ,	
14	317 F.3d 1097 (9th Cir. 2003).....	12, 14
15	<b>Statutes</b>	
16	FTC Act, 15 U.S.C. § 45 .....	3, 4
17	Cal. Civ. Code § 1798.150 .....	4, 11
18	Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101 .....	13
19	Consumer Protection Act, Tex. Bus. & Com. Code Ann. § 17.41, . .....	13
20	Illinois’s Consumer Fraud and Deceptive Business Practices Act, 805 Ill. Comp.	
21	Stat. 505/1 .....	13
22	New York General Business Law § 349 .....	13
23	Texas Deceptive Trade Practices—Consumer Protection Act, Tex. Bus. & Com.	
24	Code Ann. § 17.41 .....	13
25	<b>Rules</b>	
26	Fed. R. Civ. P. 9(b) .....	1, 12, 14
27	Fed. R. Civ. P. 12(b)(6).....	1, 3
28	Civil L.R. 7-4(a)(3) .....	1
	<b>Other Authorities</b>	
	<a href="https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf">https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf</a> .....	1, 6

**I. SUMMARY OF ARGUMENT (STANDING ORDER I.C)**

Blackhawk Network, Inc. (“Blackhawk”) is a company located in California that operates a website, [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com), that allows recipients of prepaid cards to activate and manage their cards. Blackhawk does not charge cardholders any fees for this service. On September 11, 2022, Blackhawk discovered irregular activity on [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com), which it promptly investigated and shut down the next day. Because of Blackhawk’s swift action, the scope of the irregular activity was contained—it persisted for only a short period of time, from September 4 to September 12, 2022, and involved the unauthorized acquisition of only limited information relating to certain individuals’ prepaid cards. Additionally, Blackhawk ensured that even that limited harm was quickly remedied. It promptly blocked all impacted gift cards so they could not be used and reissued new cards to the proper holders; and for any gift cards that had been used improperly in the intervening time, Blackhawk issued refunds for the affected amounts.

Nevertheless, Plaintiffs, six residents of Colorado, Mississippi, New York, Texas, California, and Illinois, seek to maintain this putative class action against Blackhawk—and insist that they are entitled to recover more than \$5 million as a result of the security event. For starters, much of Plaintiffs’ Complaint is irrelevant to this case—it is instead filled with boilerplate allegations, such as general discussions of harm that can arise from paying for a product or service that is accompanied by inadequate data security, even though the Complaint does not (and cannot) allege that any Plaintiff paid Blackhawk anything here.

That failure to plead relevant facts is not just about the inclusion of irrelevant material—it also cuts to the substantive core of Plaintiffs’ lawsuit. The basic theory of Plaintiffs’ ten causes of action is that Blackhawk “refus[ed] to take adequate and reasonable measures to ensure its data systems were protected.” Compl. ¶ 11. But the Complaint fails to identify any security measure that Blackhawk reasonably should have undertaken, or any actual actions it purportedly refused to take, which would have prevented the security event. What is more, Plaintiffs maintain that they are entitled to damages, but nowhere do they identify any cognizable harm that they have suffered as a result of the security event. Indeed, quite the opposite: for the single Plaintiff alleged to have had funds debited without authorization from his prepaid cards, he admits that Blackhawk refunded

1 those funds. Ultimately, the Complaint here is little more than a set of generalized allegations,  
2 seemingly lifted from other data security lawsuits, in hopes that they are close enough to get the  
3 job done here.<sup>1</sup> And even if the Complaint were to sufficiently plead Blackhawk's conduct (it does  
4 not), Plaintiffs' inability to articulate any cognizable harms they allegedly suffered dooms it.  
5 Plaintiffs have paid nothing to Blackhawk to use its free service, and Blackhawk has already  
6 reimbursed them for amounts that were impacted by the security event. For these various reasons,  
7 the Complaint should be dismissed in its entirety.

---

26 <sup>1</sup> *Cf. Licea v. Caraway Home Inc.*, 2023 WL 1999496, at \*6 (C.D. Cal. 2023) (noting that while it  
27 may be "easier and cheaper to copy and paste a complaint over and over again," perhaps in hopes  
28 that "a defendant is willing to offer a quick cash settlement," "legitimate litigation" "generally  
requires" more, as the complaint "must plead specific facts arising out of a specific encounter  
with a specific defendant")



1 **II. STATEMENT OF ISSUES TO BE DECIDED (CIVIL L.R. 7-4(a)(3))**

2 Whether Plaintiffs' Complaint should be dismissed for failure to state a claim under Federal  
3 Rules of Civil Procedure 12(b)(6) and 9(b).

4 **III. SUMMARY OF RELEVANT FACTS**

5 Blackhawk Network, Inc. ("Blackhawk") is a company located in California that operates  
6 a website, [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com), that allows recipients of prepaid cards to activate and  
7 manage their cards. Compl. ¶¶ 2-4. The website [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com) does not sell prepaid  
8 cards, nor does it sell goods or services to be purchased with prepaid cards. Instead,  
9 [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com) serves a single, basic function: to aid prepaid card recipients with  
10 activating their prepaid cards (so that they can then be used to make purchases from other  
11 companies) and check their card balances. *See* Compl. ¶ 4. Prepaid card holders, such as Plaintiffs,  
12 who activate and manage their cards on [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com) do not pay any money to  
13 Blackhawk for its services.

14 On September 11, 2022, Blackhawk discovered irregular activity on  
15 [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com). Compl. ¶ 12. Blackhawk promptly investigated, and stopped the  
16 irregular activity the next day. *Id.* Blackhawk's investigation revealed that the irregular activity  
17 involved the unauthorized acquisition of certain information, which occurred in a short period  
18 beginning on September 4, 2022 and ending on September 12, 2022, after Blackhawk identified  
19 the issue and remediated it. *Id.* The information affected comprised certain individuals' first and  
20 last names, email addresses, and phone numbers, as well as information relating to certain prepaid  
21 cards, such as card numbers, expiration dates, and CVV codes. *Id.* Blackhawk promptly provided  
22 notice of the irregular activity on October 31, 2022. *Id.*

23 Blackhawk also promptly blocked all impacted prepaid cards so they could not be used, and  
24 moreover reissued new cards, so that the proper holders could continue to use their funds. *See*  
25 <https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf>, *cited at, e.g.*,  
26 Compl. ¶ 9. Blackhawk also reported the incident to law enforcement. *Id.* And, it provided affected  
27 individuals with instructions for checking the balance on their gift cards through  
28 [www.MyPrepaidCenter.com](http://www.MyPrepaidCenter.com), and for reporting any unrecognized activity to Blackhawk's customer

1 support for assistance. *Id.* Where funds were improperly used, Blackhawk issued refunds for the  
 2 affected amounts. *See id.* at ¶¶ 89-90.

3 On November 11, 2022, Plaintiff Steven Pryor filed a putative class action lawsuit against  
 4 Blackhawk alleging various causes of action arising out of the security event. Five days later,  
 5 Plaintiff Sabrina Singleton filed a similar putative class action. Nearly two weeks later, on  
 6 November 28, 2022, Plaintiff Silvia Cortez (along with more than a dozen other individuals) filed  
 7 a third putative class action. On January 10, with the consent of the parties, the Court consolidated  
 8 the three actions. On February 9, 2023, Plaintiffs (the three individuals named above, plus Shane  
 9 Scheib, Brian O'Connor, and Kelly Rogers) filed their Amended Class Action Complaint. Although  
 10 the Complaint does not identify any un-refunded losses that any Plaintiff has suffered because of  
 11 the security event—or indeed, any specific security measure that Blackhawk unreasonably failed  
 12 to take to prevent the incident—Plaintiffs nevertheless maintain that they are entitled to be paid  
 13 more than \$5 million as a result of the event. Compl. ¶ 21.

#### 14 **IV. LEGAL STANDARD**

15 To survive a motion under Rule 12(b)(6), “a complaint must contain sufficient factual  
 16 matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556  
 17 U.S. 662, 678 (2009). Facial plausibility requires that there be sufficient factual allegations from  
 18 which “to draw the reasonable inference that the defendant is liable for the misconduct alleged.”  
 19 *Id.* “[L]abels and conclusions, and a formulaic recitation of the elements” of claims will not suffice.  
 20 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A court must take all of the well-pled factual  
 21 allegations in the complaint as true but is “not bound to accept as true a legal conclusion couched  
 22 as a factual allegation.” *Id.* (quoting *Papasan v. Allain*, 478 U.S. 265, 286 (1986)).

#### 23 **V. ARGUMENT**

##### 24 **A. The Complaint Fails To State A Claim For Negligence.**

25 The Complaint fails state a claim for negligence because it fails to plead facts showing  
 26 either (1) that Blackhawk was negligent—*i.e.*, that Blackhawk “breached [a] duty” that it owed to  
 27 Plaintiffs to “conform to a certain standard of conduct for the protection ... against unreasonable  
 28 risks,” *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at

1 \*3 (S.D. Cal. 2020)—or (2) that Plaintiffs suffered legally cognizable damages as a result.

2 1. *Plaintiffs fail to plead facts showing that Blackhawk was negligent.*

3 To maintain a negligence claim, Plaintiffs must plead facts showing that Blackhawk failed  
4 to meet a specific standard of care that it was legally obligated to comply with. “[B]ald allegation[s]  
5 that defendants owed plaintiffs a duty, and breached that duty” are not enough. *Jasso v. Citizens*  
6 *Telecomms. Co. of Cal.*, 2007 WL 97036, at \*5 (E.D. Cal. 2007). Rather “plaintiffs must be clear  
7 on the relevant standard of care applicable here, the source of that standard, and what factual  
8 allegations show that the duty was breached.” *Id.*; *see also Razuki v. Caliber Home Loans, Inc.*,  
9 2018 WL 6018361, at \*1 (S.D. Cal. 2018) (dismissing data-breach negligence claim because  
10 plaintiff “could have identified what made [the defendant’s] security measures unreasonable by  
11 comparison to what other companies are doing” but did not). Plaintiffs do none of those things.

12 Nearly all that the Complaint offers are bald allegations. Almost the entirety of the  
13 Complaint’s allegation are pitched at an exceedingly high level of generality, maintaining that  
14 Blackhawk “owed a duty of care not to subject Plaintiffs ... to an unreasonable risk of harm,” and  
15 “breached [that] dut[y] by failing to provide fair, reasonable, or adequate computer systems and  
16 data security practices to safeguard” their information. Compl. ¶¶ 165, 169; *see also, e.g.*, Compl.  
17 ¶ 174 (alleging that Blackhawk failed to “[s]ecure its e-commerce website”). But that “formulaic  
18 recitation of the elements” of a negligence claim is nothing but a “conclusory” allegation that is  
19 “not entitled to be assumed true” on a motion to dismiss. *Iqbal*, 556 U.S. at 680-81. What is more,  
20 the Complaint fails to plead facts establishing that Blackhawk, in fact, owed Plaintiffs such a duty  
21 (even at that high level). The Complaint relies primarily on platitudes, such as “[t]his duty is  
22 inherent in the nature of the exchange of the highly sensitive Private Information here, particularly  
23 where digital transactions are involved.” Compl. ¶ 29; *see also id.* at ¶ 162 (“By collecting this data  
24 and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure  
25 and safeguard [it].”). But those high-level assertions say nothing about the standard of care that is  
26 required, from where it originates, or why it applies to Blackhawk here. *See Jasso*, 2007 WL 97036,  
27 at \*5. The closest the Complaint gets on that score is its *en passant* invocation of the FTC Act, 15  
28 U.S.C. § 45. *See* Compl. ¶¶ 175, 236-37. But courts have been clear that the FTC Act cannot be

1 used to supply the duty for a negligence claim, because the FTC Act “creates no private right of  
 2 action,” meaning that a negligence claim based on it “is barred.” *Pica v. Delta Air Lines, Inc.*, 2018  
 3 WL 5861362, at \*9 (C.D. Cal. 2018).<sup>2</sup>

4 Just as important, even if the Complaint had shown that Blackhawk owed Plaintiffs a duty,  
 5 nowhere does it allege facts showing that Blackhawk’s security controls or measures were  
 6 unreasonable. Instead, the Complaint baldly asserts that Defendant’s security “must have been  
 7 inadequate” *because* data was accessed unlawfully. *See* Compl. ¶ 174 (alleging that Blackhawk  
 8 was negligent because it failed to “[i]mplement the systems, policies, and procedures necessary to  
 9 prevent this type of data breach”). Courts routinely hold that allegations like these—“naked  
 10 assertions devoid of [the] further factual enhancement”—should be dismissed. *Kuhns v. Scottrade,*  
 11 *Inc.*, 868 F.3d 711, 717 (8th Cir. 2017); *Razuki*, 2018 WL 6018361, at \*2 (surviving motion to  
 12 dismiss requires more than conclusory assertions and “recit[ing] a few buzz words”).

13 On the few occasions where the Complaint does offer allegations about specific security  
 14 measures, they are facially unconnected to www.MyPrepaidCenter.com. That is, the Complaint  
 15 fails to allege facts showing that any of the security measures it mentions are even applicable to  
 16 www.MyPrepaidCenter.com, much less that adopting any of them would have prevented the  
 17 exposure of Plaintiffs’ information. Specifically, the security measures mentioned in the Complaint  
 18 are related to the processing of “debit or credit card purchase *transaction[s]*,” when “card data must  
 19 flow through multiple systems and parties to be processed.” Compl. ¶ 45 (emphasis added). But  
 20 Plaintiff does not allege that www.MyPrepaidCenter.com is used for purchase transactions. Instead,  
 21 it alleges only that the website it used for “activat[ing] and manag[ing] certain prepaid” cards.  
 22 Compl. ¶ 3. Accordingly, there is nothing in the Complaint pleading that the security measures  
 23 relating to purchase transactions are applicable here at all. Put another way, while those security

---

24 <sup>2</sup> Although the Complaint elsewhere alleges that Blackhawk violated the CCPA, Cal. Civ. Code  
 25 § 1798.150, it notably *does not* allege that the CCPA gives rise to any duty that could support  
 26 Plaintiffs’ negligence claims. *See, e.g.,* Compl. ¶¶ 236-37 (discussing a “duty” created by the  
 27 CCPA only in the context of that claim, in a portion of the Complaint not incorporated by  
 28 reference into the negligence claim). In any event, even if Plaintiffs had alleged that the CCPA  
 created a duty to support their negligence claims, that would still fail—at a minimum—because  
 Plaintiffs assert their negligence claim on behalf of a nationwide class, whereas “the CCPA does  
 not apply to non-California residents.” *Hayden v. Retail Equation, Inc.*, 2022 WL 2254461, at \*5  
 (C.D. Cal. 2022).

measures are all fine and well, the Complaint fails to plead that they were required or applied to www.MyPrepaidCenter.com. Still more, because the Complaint does not identify any applicable security measures that Blackhawk unreasonably failed to take, it also fails to allege facts showing that Plaintiffs' injuries were *caused* by any (unspecified) failure. Indeed, even if Plaintiffs rectified all of the pleading defects identified above (and they have given no reason to think they can), their claims would still fail for lack of any allegations that an absent security control identified by Plaintiffs have caused the incident.

In short, the Complaint contains no allegations identifying any act that Blackhawk unreasonably took, or failed to take, that would have caused the security incident that is the subject of Plaintiffs' claims. Accordingly, for this reason alone, it fails to state a claim for negligence.

2. *Plaintiffs fail to plead facts showing that they suffered cognizable injury.*

Plaintiffs list nine types of injuries they allegedly suffered because of the security event. Compl. ¶ 12. But many of those claimed injuries are affirmatively refuted by Plaintiffs' other (more specific) allegations, and the few that do remain are not legally cognizable in a negligence action:

a. *Unauthorized charges on their payment card accounts.* Plaintiffs' primary claim of injury rests on "[u]nauthorized charges," but only a single Plaintiff (Scheib) alleges that he suffered this harm. Compl. ¶ 91. Critically, however, that Plaintiff admits that he has already been "reimbursed for" this injury. Compl. ¶ 90. There are thus no Plaintiffs who allege they are currently suffering any "un-reimbursed charges" because of the security event. That means this claimed harm "cannot satisfy the necessary damage element of a negligence claim." *Aguilar v. Hartford Accident & Indem. Co.*, 2019 WL 2912861, at \*2 (C.D. Cal. 2019) (quoting *In re Sony Gaming Networks and Customer Data Sec. Breach Litigation*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012)).

b. *Theft of personal and financial information.* Courts have been clear that the mere "loss of privacy engendered by an accidental data breach" standing alone "cannot satisfy the necessary element of a negligence claim." *Aguilar*, 2019 WL 2912861, at \*2. Rather, to sustain a negligence claim Plaintiffs must plead "specific factual statements that [their] Personal Information has been misused" (and in a way that results in a harm that remains "un-reimbursed"). *Id.* Nowhere do Plaintiffs allege misuses of personal or financial information.

1           c.       *Costs associated with detection and prevention of identity theft.* As with the  
 2 “unauthorized charges” harm discussed above, although Plaintiffs frame this injury broadly, only a  
 3 single Plaintiff (Scheib) actually alleges that he paid for any identity theft prevention or detection  
 4 services. *See* Compl. ¶ 97. But even as to Plaintiff Scheib, the Complaint fails to allege facts  
 5 showing that this cost is recoverable. That is because “the costs of credit monitoring after a data  
 6 breach are recoverable in negligence” only if the plaintiff pleads facts showing that the monitoring  
 7 costs were “both reasonable and necessary.” *In re Sony Gaming Networks & Customer Data Sec.*  
 8 *Breach Litig.*, 996 F.Supp.2d 942, 970 (S.D. Cal. 2014). “[T]his is a high burden and requires a  
 9 plaintiff to plead both a logical and temporal connection between the decision to purchase credit  
 10 monitoring services and the defendant’s alleged breach.” *Id.* The Complaint contains no such facts.  
 11 It does not allege when Plaintiff Scheib purchased his credit monitoring services, or why his  
 12 decision to do so was reasonable given the information affected by the security event. That absence  
 13 of allegations is unsurprising. As the Complaint itself makes clear, the affected information  
 14 involved “first and last name, email address, and phone number” as well as information specific to  
 15 prepaid cards (which Blackhawk blocked from use). Compl. ¶ 9; *see also* [https://dojmt.gov/wp-](https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf)  
 16 [content/uploads/Consumer-Notification-Letter-675.pdf](https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf) (cited at *id.*). There is no logical  
 17 explanation—and the Complaint provides none—for how that limited information could create a  
 18 risk of identity theft sufficient to justify Plaintiff Scheib’s decision to purchase credit monitoring  
 19 services. Accordingly this claim of injury, too, cannot sustain Plaintiffs’ negligence claim.

20           d.       *Loss of use of and access to their account funds.* The Complaint’s general invocation  
 21 of various harms flowing from “the inability to obtain money from [gift card] accounts”, “including  
 22 missed payments on bills and loans, late charges and fees, and ... decreased credit scores,” can be  
 23 swiftly disregarded. *See* Compl. ¶ 12. No Plaintiff actually claims to have suffered those harms.  
 24 Accordingly, they cannot serve as a basis for recovery in this suit. *See Sanford v. MemberWorks,*  
 25 *Inc.*, 625 F.3d 550, 560 (9th Cir. 2010) (holding that because the named plaintiff had “no cognizable  
 26 claim for relief,” she could not “represent others who may have such a claim” in a class action,  
 27 even if some member of the putative class did suffer the harm alleged); *Rudgayzer v. Yahoo! Inc.*,  
 28 2012 WL 5471149, at \*3 (N.D. Cal. 2012) (“[I]f none of the named plaintiffs purporting to

1 represent a class establishes the requisite of a case or controversy with the defendants, none may  
 2 seek relief on behalf of himself or any other member of the class.”).

3 *e. Lost time spent addressing the security event.* Plaintiffs’ attempt to recover for “time  
 4 spent ... to address and attempt[] to ameliorate ... the actual and future consequences of the data  
 5 breach,” Compl. ¶ 12, runs headlong into the caselaw holding that “general allegations of lost time”  
 6 fail to “constitute cognizable injury” in a negligence action. *also Corona v. Sony Pictures Ent., Inc.*,  
 7 2015 WL 3916744, at \*4 (C.D. Cal. 2015). Therefore, this alleged injury also cannot sustain  
 8 Plaintiffs’ negligence claim.

9 *f. Potential theft, fraud, and identity theft.* Plaintiffs’ argument that they can collect  
 10 for injuries that they have not suffered, but may hypothetically suffer in the future, similarly runs  
 11 directly contrary to the caselaw holding that “the threat of future harm” does not “suffice to create  
 12 a cause of action for negligence.” *In re Sony Gaming Networks*, 903 F. Supp. 2d at 962-63; *see also*  
 13 *Corona*, 2015 WL 3916744, at \*3 (“[T]he mere threat of future harm is insufficient to constitute  
 14 actual loss[.]”) (citing *Jordache Enters., Inc. v. Brobeck, Pheger & Harrison*, 18 Cal. 4th 739  
 15 (1998)); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009), *aff’d*, 380 F. App’x 689 (9th  
 16 Cir. 2010) (risk of future harm “does not rise to the level of appreciable harm necessary to assert a  
 17 negligence claim”).<sup>3</sup> It cannot form the basis of Plaintiff’s suit.

18 *g. Diminution in the value of Plaintiffs’ personal information.* Plaintiffs claim that the  
 19 value of their personal information was diminished when Blackhawk “allow[ed] access” to it “by  
 20 others.” Compl. ¶ 12. But the Complaint is entirely devoid of allegations showing either that the  
 21 personal information at issue here—name, email address, and phone number—had any appreciable  
 22 value prior to the security incident, or that the incident caused that value to decrease. No wonder,  
 23 as most of that information is largely public or freely available in any event.<sup>4</sup> Ultimately, that lack

24 <sup>3</sup> The Complaint also occasionally gestures at “anxiety” that Plaintiffs have supposedly suffered  
 25 about the potential for future harms. *See, e.g.*, Compl. ¶ 83. The law is clear, however, that mental  
 26 and emotional distress are not actionable in negligence absent an assumption of duty “in which  
 27 the emotional condition of the plaintiff is an object.” *Erlich v. Menezes*, 21 Cal. 4th 543, 554–55  
 (1999). And even then, the distress must still arise from “physical injury, not simply damage to  
 property or financial interests.” *Id.* Plaintiffs have not pled any such duty, nor do they claim to  
 have suffered physical injury, so their attempt to recover for emotional distress fails.

28 <sup>4</sup> To the extent Plaintiffs mean to suggest that their prepaid card numbers and CVVs diminished  
 in value, that makes no sense either. That information has value only to the extent it allows a



1 of factual allegations is fatal, as courts have not recognized “authority that an individual’s personal  
 2 identifying information has any compensable value in the economy at large.” *Corona*, 2015 WL  
 3 3916744, at \*4 (rejecting attempt to predicate negligence claim on a supposed diminution of value  
 4 of personal information for that reason); *see also, e.g., Adkins v. Facebook, Inc.*, 424 F. Supp. 3d  
 5 686, 697 (N.D. Cal. 2019) (finding alleged diminution in value of personal information insufficient  
 6 for negligence claim because even if personal information is valuable to companies, “it does not  
 7 follow that the same information has independent economic value to an individual user”). Absent  
 8 some factual allegation establishing that the personal information at issue here is somehow different  
 9 from prevailing caselaw, Plaintiffs’ claimed diminution in value of their personal information  
 10 cannot sustain a negligence claim.

11 *h. Overpayment to Blackhawk.* Plaintiffs claim that had they understood that  
 12 Blackhawk “lacked adequate systems and procedures to reasonably safeguard [their] Private  
 13 Information,” they “would have paid less for [Blackhawk’s] services or products.” Compl. ¶ 12.  
 14 But Plaintiffs do not actually allege that they paid Blackhawk *anything* at all. And so even on its  
 15 own terms, this theory fails to establish that Plaintiffs have suffered any damages. For this reason  
 16 alone, Plaintiffs’ claimed overpayment harm should be dismissed. *See In re Google Assistant Priv.*  
 17 *Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) (“[I]t cannot be said that Plaintiffs received less  
 18 than what they paid for—they appeared to have paid nothing.”); *In re LinkedIn User Privacy Litig.*,  
 19 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (rejecting plaintiffs’ benefit of the bargain theory  
 20 because “the FAC fails to allege that Plaintiffs actually provided consideration for the security  
 21 services which they claim were not provided”).

22 *i. Continued risk to Plaintiffs’ information.* Plaintiffs’ final claim of injury—from the  
 23 “[c]ontinued risk to their” information, Compl. ¶ 12—is just a repeat of the earlier-claimed harm  
 24 about the potential of future injuries. *See* Section IV.A.2.f, *supra*. And so it runs into exactly the  
 25 same caselaw holding that “the mere threat of future harm is insufficient to constitute actual loss.”

26 \_\_\_\_\_  
 27 person to access the funds associated with those numbers. And here Blackhawk already blocked  
 28 affected cards, reissued new ones (with new numbers and CVVs), and reimbursed affected  
 amounts—meaning that to the extent Plaintiffs’ numbers and CVVs were affected at all, they  
 have already been provided with new ones that retain exactly the same value as their old ones.



1 *Corona*, 2015 WL 3916744, at \*3 (citing *Jordache*, 18 Cal. 4th 739); *In re Sony Gaming Networks*,  
 2 903 F. Supp. 2d at 962-63; *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009), *aff'd*, 380  
 3 F. App'x 689 (9th Cir. 2010).

4 Plaintiffs have thus failed to plead facts showing either that Blackhawk was negligent—*i.e.*,  
 5 that it failed to take reasonable security measures—or that Plaintiffs have suffered any legally  
 6 cognizable injury. Their negligence claim must be dismissed.

7 **B. Plaintiffs fail to state a claim for breach of implied contract.**

8 Plaintiffs' breach of implied contract claim fails for at least two independent reasons. First,  
 9 Plaintiffs' claim of an implied contract rests on Plaintiffs' assertion that when Blackhawk "invited  
 10 its customers ... to make purchases of Prepaid Gift cards on its website," an "implicit part of th[at]  
 11 offer was that Defendant would safeguard their Private Information."<sup>5</sup> Compl. ¶¶ 184-185. But that  
 12 theory fails to apply to Plaintiffs here, as none alleges that they "ma[d]e purchases of Prepaid Gift  
 13 cards on [Blackhawk's] website." (In fact, none could make such an allegation, as Blackhawk's  
 14 website, MyPrepaidCenter.com, does not allow for such purchases.) And so, even on its own terms,  
 15 Plaintiffs' implied-contract theory fails because Plaintiffs do not allege that any of them accepted  
 16 an implicit offer (that Blackhawk never made).

17 Second, even if Plaintiffs had alleged facts showing that they had formed an implied  
 18 contract with Blackhawk, their claim would still fail. That is because courts, including this Court,  
 19 view an implied contract claim to be essentially the same as a "benefit of the bargain" or  
 20 "overpayment" theory in a negligence action. *See, e.g., Ortiz v. Perkins & Co.*, 2022 WL 16637993,  
 21 at \*6 (N.D. Cal. 2022). Such a theory would require the plaintiff to allege "that [the defendant]  
 22 represented in [its] Privacy Policy, or otherwise, that the cost of data security was included in the  
 23 cost of its goods." *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at \*6 (N.D. Cal. 2021). Said  
 24 otherwise, Plaintiffs need to do more than just assert that some portion of what they paid *must have*

---

25  
 26 <sup>5</sup> To the extent Plaintiffs attempt to rely on Blackhawk's Privacy Policy as a source of an implied  
 27 contract, that runs headlong into the caselaw. As courts have recognized, a Privacy Policy is  
 28 typically not a contract, but rather a "unilateral statement of company policy." *Gardner v. Health*  
*Net, Inc.*, 2010 WL 11597979, at \*6 (C.D. Cal. 2010). And so absent allegations of specific facts  
 showing why the "Privacy Policy [here] was anything more," Plaintiffs cannot use that Policy to  
 maintain a breach of contract claim. *Id.*

1 been for data security; instead, they must provide specific “information to show” that they in fact  
 2 “paid a premium for [Blackhawk] to provide reasonable and adequate security measures.” *Razuki*,  
 3 2018 WL 6018361, at \*1. Here, this claim fails at its incept because Plaintiffs do not (and cannot)  
 4 allege that they paid anything for the services offered at www.MyPrepaidCenter.com. It further  
 5 fails because, even if there was a so-called “purchase”, the Complaint lacks any allegations showing  
 6 how Plaintiffs’ “purchases included a sum understood by the parties to be allocated toward  
 7 customer data protection.” *Gardiner*, 2021 WL 2520103, at \*6. Accordingly, they cannot recover  
 8 on an overpayment theory, and hence cannot recover for a breach of implied contract.

9 **C. Plaintiffs fail to state a claim for unjust enrichment.**

10 Plaintiffs’ unjust enrichment claim fails for the same reasons. Plaintiffs’ basic theory is that  
 11 Blackhawk was unjustly enriched because Plaintiffs “conferred a monetary benefit on Defendant,”  
 12 by “purchas[ing] goods (Prepaid Gift Cards, specifically) and services from Defendant and in so  
 13 doing provid[ed] Defendant with their Private Information.” Compl. ¶ 199. As noted above,  
 14 however, Plaintiffs do not actually allege that they “purchased goods ... and services”—or indeed,  
 15 anything—from Blackhawk. *See* Section IV.B, *supra*. As a result, Plaintiffs have failed to allege  
 16 that they have conferred any enrichment (much less an unjust one) on Blackhawk at all. Having  
 17 “fail[ed] to identify any benefit that [Blackhawk] retained” unjustly, Plaintiffs’ unjust-enrichment  
 18 claim must be dismissed.” *Ortiz v. Perkins & Co.*, 2022 WL 16637993, at \*7 (N.D. Cal. 2022).

19 **D. Plaintiffs fail to state a claim under the UCL.**

20 A similar defect also plagues Plaintiffs’ UCL claim. To maintain a claim under the UCL, a  
 21 plaintiff must plead facts establishing (among other things) “a loss or deprivation of money or  
 22 property sufficient to qualify as injury in fact, i.e., economic injury.” *Kwikset Corp. v. Super. Ct.*,  
 23 51 Cal. 4th 310, 322 (2011). Plaintiffs claim they have satisfied that requirement because they (1)  
 24 “paid an unwarranted premium for the purchased services” (“[s]pecifically,” they say they “paid  
 25 for services advertised as secure”); and (2) “relied on and made their decision to use [Blackhawk]’s  
 26 services in part based on [Blackhawk]’s representations regarding [its] security measures.” Compl.  
 27 ¶ 222. But Plaintiffs’ first argument fails, because (as explained above) Plaintiffs do not, and  
 28 cannot, allege that they paid *anything* to Blackhawk—and so cannot maintain a UCL claim based

on these non-existent payments. Plaintiffs’ second theory fails because the mere “decision to use [Blackhawk’s] services”—which, again, Plaintiffs did not pay for—is not a loss of “money or property” as the UCL requires.<sup>6</sup> Plaintiffs may mean to suggest that if they had correctly understood Blackhawk’s security, they would have avoided using Blackhawk’s service and their personal information would not have been exposed. But, that argument fails because exposure of personal information is not a loss of “money or property.” See *In re Sony Gaming Networks*, 903 F. Supp. 2d at 965-66 (mere fact that plaintiffs’ “Personal Information was compromised” is not “a cognizable injury” under the UCL because it does not reflect “lost money or property”); *In re iPhone Application Litig.*, 2011 WL 4403963, at \*14 (N.D. Cal. 2011) (“Numerous courts have held that a plaintiff’s ‘personal information’ does not constitute money or property under the UCL.”). Nor can Plaintiffs manufacture this into a cognizable injury, through the other vague, inchoate, and unsupported claims of harm that they make elsewhere in their Complaint (but do not discuss in their UCL claim). See, e.g., *In re Sony Gaming Networks*, 903 F. Supp. 2d at 966 (“Plaintiffs’ allegations that the heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one’s information, do not suffice as injury under the UCL.”); *Ruiz v. Gap, Inc.*, 2009 WL 250481 at \*3–4 (N.D. Cal. 2009), *aff’d*, 380 Fed. App’x at 692 (time and money spent to monitor and repair credit is not the “kind of loss of money or property necessary” to assert a claim under the UCL).<sup>7</sup>

#### **E. Plaintiffs fail to state a claim under the CCPA.**

To state a claim under the CCPA, Plaintiffs must allege facts showing that (1) as a result of Blackhawk’s failure “to implement and maintain reasonable security measures,” (2) their “nonencrypted and nonredacted personal information” was subject to unauthorized access or disclosure. Cal. Civ. Code § 1798.150(a)(1). Plaintiffs’ Complaint does not meet either of those

<sup>6</sup> As noted above, one only named Plaintiff (Scheib) alleged that he had lost money as a result of the security incident, but he is not a member of the California subclass on whose behalf the UCL claim is asserted. What is more, he concedes that that money has already been refunded to him.

<sup>7</sup> Although Plaintiffs state that they intend to bring this claim “[f]or all Class members outside of” any State in which a named Plaintiff resides, “under the relevant consumer protection statute for the state in which they reside,” Compl. ¶ 208, that effort fails. “Where, as here, a representative plaintiff is lacking for a particular state, all claims based on that state’s laws are subject to dismissal.” *In re Flash Memory Antitrust Litig.*, 643 F. Supp. 2d 1133, 1164 (N.D. Cal. 2009).

requirements here. As explained above, the Complaint has no factual allegations establishing any specific failure by Blackhawk to take reasonable security measures. While Plaintiffs allege a laundry list of measures that Blackhawk allegedly did not take, not a single one is connected to the event; i.e., there is no allegation that any of those caused the event. That is, there is no allegation that had Blackhawk taken one (or more) of those measures that the event would have been prevented. And so for all the same reasons Plaintiffs fail to show that Blackhawk acted negligently (i.e., unreasonably), they also fail to state a CCPA claim. *See Danfer-Klaben v. JPMorgan Chase Bank, N.A.*, 2022 WL 3012528, at \*7 (C.D. Cal. 2022) (dismissing CCPA claim because plaintiff failed to allege that “Defendant's disclosure to third parties was the result of a failure ‘to implement and maintain reasonable security measures’”).

**F. Plaintiffs fail to state a claim for deceit by concealment.**

To establish deceit by concealment, Plaintiffs must demonstrate, among other things: (1) that Blackhawk concealed or suppressed a fact that it was under a duty to disclose to them, and (2) that Blackhawk did so with the intent to defraud the plaintiffs. *Tae Youn Shim v. Lawler*, 2019 WL 2996443, at \*17 (N.D. Cal. 2019). What is more, because deceit by concealment “sounds in fraud” and is therefore subject to Rule 9(b)’s heightened pleading standard, Plaintiffs must plead facts showing the above elements “with particularity.” *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 800 (N.D. Cal. 2019); *see also, e.g., Brisson v. Bayer Corp.*, 2013 WL 12097794, at \*5 (S.D. Cal. 2013) (dismissing fraud-based claims, including deceit by concealment, “[b]ecause the complaint does not satisfy Rule 9(b)’s [particularity] requirement”). Rule 9(b) requires a party to “state with particularity the circumstances constituting fraud or mistake,” Fed. R. Civ. P. 9(b), including “the who, what, when, where, and how of the misconduct charged,” *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103–05 (9th Cir. 2003). For that reason alone—the failure to comply with Rule 9(b)—this claim should be dismissed. But there are two more substantive reasons for dismissal, as well.

First, Plaintiffs fail to allege any facts supporting their conclusory assertion that Blackhawk had a duty “to disclose to consumers that its security systems were not adequate to safeguard their

Private Information.”<sup>8</sup> Compl. ¶ 250. A duty to disclose arises in only four circumstances: “(1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material facts.” *Terpin v. AT&T Mobility, LLC*, 2020 WL 5369410, at \*3 (C.D. Cal. 2020) (quoting *LiMandri v. Judkins*, 52 Cal. App. 4th 326, 336 (1997)). The Complaint, however, supplies no allegations that establish any of those here. Rather, the Complaint’s theory is that Blackhawk’s duty to disclose arose out of the fact that—years earlier—it experienced a *separate* security event involving *different* information. Compl. ¶ 249. But Plaintiffs offer no explanation (nor is any apparent) for how a years-old, fully resolved, and wholly unrelated security incident could give rise to a duty to disclose.

Second, Plaintiffs fail to allege facts showing that Blackhawk’s alleged non-disclosures were “intentional[]” and done “with the intent to defraud the plaintiff.” *Terpin*, 2020 WL 5369410, at \*3. Indeed, the Complaint offers no allegations on that score whatsoever. Accordingly, for this reason too, Plaintiffs’ deceit by concealment claim must be dismissed. *See MyGo, LLC v. Mission Beach Indus., LLC*, 2017 WL 107346, at \*6 (S.D. Cal. 2017) (allegations failed to show requisite intent to deceive when they “provide[d] neither the information on which [they] relie[d] nor any plausible reasons for [their] belief”).

**G. Plaintiffs fail to state a claim under various state consumer protection statutes.**

Plaintiffs allege purported violations of four state consumer protection statutes: (1) Illinois’s Consumer Fraud and Deceptive Business Practices Act, 805 Ill. Comp. Stat. 505/1, *et seq.*; (2) Texas’s Deceptive Trade Practices—Consumer Protection Act, Tex. Bus. & Com. Code Ann. § 17.41, *et seq.*; (3) Colorado’s Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*; and (4) New York’s General Business Law § 349. But Plaintiffs’ claims under the consumer protection statutes all fail for the same reason as their negligence claim. The gravamen of each of Plaintiffs’

---

<sup>8</sup> The Complaint also states in passing that Blackhawk “waited over a month” after discovering the security event “before announcing it to the public.” Compl. ¶ 250. But because the Complaint does not allege that Blackhawk had any duty to disclose the security event any sooner, this aside is irrelevant to (and cannot serve as a basis for) Plaintiffs’ deceit by concealment claim.

1 consumer-protection claims is that Blackhawk engaged in “deceptive” conduct by “[f]ailing to  
 2 implement and maintain reasonable security and privacy measures,” while “[m]isrepresenting that  
 3 it” had, in fact, “implement[ed] and maintain[ed] reasonable security measures.” Compl. ¶¶ 260,  
 4 264 (Illinois); *id.* ¶¶ 278a, e (Texas); *id.* ¶¶ 293a-c (Colorado); *id.* ¶¶ 301a, d (New York). As  
 5 explained above, the Complaint is absent of allegations actually establishing that Blackhawk’s  
 6 security measures were unreasonable. And so that same deficiency sinks these claims as well.

7 In fact, the Complaint’s shortcoming is even more striking here, as each of the consumer-  
 8 protection statutes here requires the claims to be pled with specificity under Rule 9(b). *See, e.g.,*  
 9 *Guajardo v. Skechers USA, Inc.*, 503 F. Supp. 3d 746, 754 (C.D. Ill. 2020) (Illinois’s Consumer  
 10 Fraud and Deceptive Business Practices Act); *Floors for Living, LLC v. MAPEI Corp.*, 2020 WL  
 11 13413204, at \*3 (S.D. Tex. 2020) (Texas Deceptive Trade Practices Act); *Monson v. Country*  
 12 *Preferred Ins. Co.*, 2018 WL 11016704, at \*2 (D. Colo. 2018) (Colorado Consumer Protection  
 13 Act); *Keegan v. Am. Honda Motor Co., Inc.*, 838 F. Supp. 2d 929, 958 (C.D. Cal. 2012) (New York  
 14 General Business Law § 349). That is because the gravamen of each of the four consumer-  
 15 protection claims sounds in fraud—namely that the business allegedly made false or deceptive  
 16 statements about its privacy and data security practices. Compl. ¶ 258 (Illinois), ¶ 277 (Texas),  
 17 ¶ 293 (Colorado), ¶ 301 (New York). And so each claim requires Plaintiffs to do more than “set  
 18 forth more than the neutral facts necessary to identify” the supposedly deceptive behavior; instead  
 19 the Complaint must state specifically “the who, what, when, where, and how” of the misconduct  
 20 charged. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). Said otherwise, the  
 21 Complaint must—at a minimum—identify with particularity each supposedly false or misleading  
 22 statement or omission, “what is false or misleading about” it, and “why it is false.” *Id.* Plaintiffs,  
 23 however, fail to identify any specific statements from Blackhawk regarding data security—much  
 24 less any allegations showing with particularity which pieces of those statements are false and why.  
 25 Plaintiffs’ consumer protection claims accordingly must be dismissed.

26 Notably, Plaintiffs’ consumer protection claims *do not* advance a separate “unfairness”  
 27  
 28

theory, distinct from the “deceptive” theory.<sup>9</sup> To the contrary, the Complaint consistently treats the two together, making only a single set of allegations (already discussed above), which it labels (repeatedly) as both “unfair ... and deceptive.” *See, e.g.*, Compl. ¶¶ 258, 259, 272, 277, 294. In any event, even if Plaintiffs had separately pled an “unfairness” theory, their causes of action would still fail, as they have not alleged the key elements of an “unfairness” claim. To the extent the Complaint speaks of an “unfairness” theory at all, the argument seems to be that Blackhawk collected data that it “did not need ... from its consumers” and then “fail[ed] to implement and maintain reasonably security measures” to protect it. Compl. ¶¶ 211-14. But like many of Plaintiffs’ other claims, this one too rests on the premise that Blackhawk unreasonably failed to implement security measures that would have prevent the security event—a premise that Plaintiffs have failed to provide any factual allegations to support. Similarly without support is Plaintiffs’ conclusory assertion that Blackhawk collected data that it “did not need.” In fact, Plaintiffs do not even attempt to explain in what way Blackhawk’s collection of their few pieces of information pled in the Complaint (name, email, phone number, and card information) was unnecessary to activating and managing Plaintiffs’ prepaid cards. More fundamentally, Plaintiffs also fail to plead facts establishing the hallmark of an unfairness claim—namely, that Blackhawk caused a “substantial injury to consumers which [was] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits.” *See, e.g., Miner v. Gov’t Payment Serv., Inc.*, 2015 WL 3528243, at \*7 (N.D. Ill. 2015). Indeed, the Complaint includes no allegations that any injury was “not reasonably avoidable” by consumers—e.g., by using a different mechanism for activating their prepaid cards. Accordingly, even if they had brought a separate unfairness claim, Plaintiffs’ consumer protection causes of action would still (for all the reasons above) have to be dismissed.

## VI. CONCLUSION

For the foregoing reasons, the Court should dismiss the Complaint with prejudice.

---

<sup>9</sup> This is in striking contrast to their UCL claim (which is not incorporated into their Illinois, Texas, Colorado, or New York claims), which *does* separate out an “unfairness” theory, *see* Compl. ¶¶ 209-22, albeit one that still fails for not only the reasons described in the UCL section above, *see supra* § IV.D, but also all the reasons in text here.



1 Dated: March 13, 2023

Respectfully Submitted,

3 /s/ Aravind Swaminathan

4 Aravind Swaminathan

Rebecca Harlow

Thomas Fu

5 ORRICK, HERRINGTON & SUTCLIFFE LLP

405 Howard Street

6 San Francisco, CA 94105

aswaminathan@orrick.com

7 Attorneys for Defendant

8 Blackhawk Networks, Inc.